POLÍTICA DE GESTÃO DA INFORMAÇÃO DA METROFOR

1. Objetivo

A Política de Gestão da Informação da METROFOR, doravante denominada "Política", tem por objetivo regular a classificação das informações segundo critérios de sigilo, definir a estrutura de classificação, orientar sobre as competências e definir responsabilidades no tratamento de informações que agregam valor à sua competitividade e que possam causar impactos no seu desempenho operacional ou financeiro, participação no mercado, imagem ou no relacionamento com as partes interessadas.

2. Abrangência

As diretrizes estabelecidas nesta Política deverão ser observadas por todas as áreas da Companhia.

3. Documentos de Referência e Complementares

3.1. Documentos de referência

- NBR ISO/IEC 17799/2001 - Tecnologia da Informação - Código de prática para a gestão da segurança da informação;
- Lei nº 15.175/2012 - Lei Estadual de Acesso à Informação;
- Lei nº 13.303/2016 - Disposições aplicáveis às empresas públicas e às sociedades de economia mista;
- Código de Conduta e Integridade da Companhia.

4. Definições

Para efeito desta Política, serão consideradas:

4.1. Informações Ultrassecretas - informações que, se reveladas, podem ocasionar danos graves e irrecuperáveis de nível político ou estratégico, comprometendo os negócios ou a imagem da Companhia, causando reflexos acionários ou ameaças a pessoas e instalações. O prazo máximo de restrição de acesso a este tipo de informação é de 25 (vinte e cinco) anos;

4.2. Informações Secretas - informações que garantem à Companhia a obtenção de vantagens competitivas; descrevem uma parte significante dos seus negócios; contêm estratégias operacionais de longo prazo; têm um impacto potencialmente sério nas políticas e práticas relacionadas a recursos humanos. O prazo máximo de restrição de acesso a este tipo de informação é de 15 (quinze) anos;

4.3. Informações Reservadas - informações que garantem à Companhia a manutenção das suas vantagens competitivas; descrevem uma parte dos seus negócios; contêm planos operacionais de curto e médio prazo. O prazo máximo de restrição de acesso a este tipo de informação é de 05 (cinco) anos;

4.4. Informações Públicas - informações da Companhia que não apresentam potencial de risco e que sua divulgação ao público externo agregue valor à competitividade do negócio e à imagem. São consideradas públicas também as informações que tem divulgação determinada por lei. As Informações Públicas podem ser disponibilizadas, desde que para o público externo alvo da informação;

4.5. Tratamento das Informações - Conjunto de procedimentos relativos ao tratamento de informações e da documentação produzida e/ou recebida pela Companhia, englobando tarefas

relativas ao recebimento, elaboração, manuseio, reprodução, divulgação, guarda, transporte, descarte e criptografia;

4.6. Cifra ou Criptografia - Sistema criptográfico constituído por um algoritmo matemático que, mediante o emprego de uma cadeia de chaves, permite transformar um texto claro em um texto ininteligível e vice-versa;

4.7. Documento Confidencial - Qualquer documento, sistema de informação ou mídia eletrônica **que contenha informação classificada**, em relação ao grau de sigilo, como **ultrassecreta ou secreta**;

4.8. Documento Reservado - Qualquer documento, sistema de informação ou mídia eletrônica que contenha informação classificada, em relação ao grau de sigilo, como reservada;

4.9. Documento Público - Qualquer documento, sistema de informação ou mídia eletrônica que contenha informação classificada, em relação ao grau de sigilo, como pública;

4.10. Documentos eletrônicos em mídia transportável - Documentos armazenados em mídias tais como CDs, DVDs, fitas magnéticas, cartuchos eletrônicos, flash memories ou qualquer outro meio eletrônico transportável que exista ou venha a ser criado;

5. Autoridade e Responsabilidade

5.1. Coordenador do Comitê Setorial de Acesso à Informação - Empregado integrante do quadro permanente da Companhia, formalmente designado pela Diretoria Executiva para coordenar as atividades de Acesso à informação;

5.2. Gestor de Segurança da Informação - Gestor da unidade organizacional que origina ou adquire a informação, tornando-se responsável pela sua segurança, ou da unidade organizacional especificamente designada como tal pelo nível gerencial competente;

5.3. Custodiante - Gestor da unidade organizacional responsável pelo armazenamento, processamento, manutenção, recuperação, disponibilização, guarda, transporte e eventual descarte da informação;

5.4. Usuário - Empregado ou contratado autorizado a utilizar informações e recursos de informação da Companhia;

5.5. Contratado - Prestador de serviços que, por contrato, deve permanecer dentro da organização por um período determinado.

6. Descrição e Diretrizes Da Política

6.1. Tratamento a ser observado nas diversas etapas de tramitação de documentos confidenciais e reservados

6.1.1. Na etapa de recebimento

Cabe aos responsáveis pelo recebimento de documentos corporativos confidenciais e reservados:

- Verificar e registrar, se for o caso, indícios de violação ou de quaisquer irregularidades na correspondência recebida, dando ciência do fato ao remetente;
- Assinar e datar o respectivo recibo que acompanha o documento, se houver;
- Proceder ao protocolo ou registro do documento em livro ou software adequado a tal finalidade, se necessário;

- Submeter documentos eletrônicos em mídia transportável a software antivírus, rejeitando-os quando verificada a sua existência, dando ciência do fato ao remetente.

6.1.2. Na etapa de elaboração

- Documentos confidenciais e reservados devem ser elaborados, necessariamente, nas instalações da Companhia, tomando-se o cuidado de protegê-los de acessos não autorizados;
- Não é permitida a elaboração de documentos confidenciais e reservados em lugares públicos.

6.1.3. Na etapa de manuseio

Documentos confidenciais e reservados devem ser manuseados, necessariamente, nas instalações da Companhia, tomando-se todos os cuidados, de modo a preservar a sua integridade e o seu sigilo.

6.1.4. Na etapa de reprodução

- É permitida a reprodução de todo ou parte de documentos confidenciais ou reservados, se autorizada pelo Gestor da Informação, devendo a cópia ter o mesmo grau de sigilo do documento original e ser autenticada pelo respectivo Gestor;
- O responsável pela reprodução de documentos confidenciais e reservados deve destruir notas, manuscritos, clichês ou quaisquer outros elementos que possam dar origem à cópia não autorizada do todo ou parte;
- A reprodução de documentos confidenciais e reservados deve ser realizada dentro de área apropriada ao seu grau de sigilo;
- Sempre que a preparação para a reprodução de documentos confidenciais e reservados for efetuada em tipografias, impressoras ou oficinas gráficas, esta operação deve ser acompanhada por pessoal oficialmente designado, a quem será imputada responsabilidade pela garantia do sigilo;
- A reprodução de documentos confidenciais e reservados em mídia eletrônica transportável somente poderá ser efetuada se autorizada pelo Gestor da Informação;
- Cada exemplar de documentos confidenciais e reservados deve conter uma numeração de controle, de modo a identificar, de forma inequívoca, o seu detentor.

6.1.5. Na etapa de divulgação

- Caso haja necessidade de divulgação para o ambiente externo, os documentos confidenciais e reservados devem ser previamente analisados pelo Comitê Setorial de Acesso à Informação e a aprovação da divulgação deve ser formalizada pelos respectivos gestores e instâncias responsáveis;
- A expedição de documentos confidenciais e reservados por meio de correio eletrônico somente poderá ocorrer mediante criptografia e com a certificação digital do emissor;
- Não é permitida a transmissão de documentos confidenciais e reservados via fax.

6.1.6. Na etapa de guarda

- Documentos confidenciais e reservados serão guardados em condições especiais de segurança, tais como armários ou gavetas com chaves e, sempre que possível, em locais de pouco trânsito de pessoas;
- A guarda de documentos confidenciais e reservados em pasta de servidor deve ser feita seguindo a orientação da ASTIG, que identificará o servidor seguro a ser usado por cada área;
- Não é permitida a guarda de documentos confidenciais e reservados em disco rígido de desktops ou laptops pessoais;

- Documentos confidenciais e reservados só podem ser guardados em discos rígidos de desktops ou laptops corporativos se criptografados, com a autorização do Gestor da Informação, e devendo uma cópia ser mantida em servidor seguro;
- Documentos confidenciais e reservados armazenados em mídia eletrônica transportável devem seguir as mesmas recomendações dos itens anteriores;
- Documentos confidenciais e reservados, inclusive aqueles gerados em meios magnéticos, devem ser guardados de forma a permitir consultas a posterior.

6.1.7. Na etapa de transporte

- É proibido o transporte de documentos confidenciais e reservados fora das instalações da Companhia, exceto aqueles autorizados pelo Gestor da Informação;
- É de responsabilidade do usuário no transporte dos documentos, sobretudo fora das instalações da Companhia, considerar a sensibilidade de seu conteúdo e avaliar os riscos relativos à sua circulação;
- Para o transporte de documentos confidenciais e reservados serão inscritos o nome e a função do destinatário, seu endereço completo e, claramente indicado, o grau de sigilo do documento;
- É permitida a expedição de documentos confidenciais e reservados pelo correio, em correspondência expressa registrada, em envelopes próprios que possuam lacre, e acondicionada em um segundo envelope que descaracterize o grau de sigilo.

6.1.8. Na etapa de descarte

- O descarte de documentos confidenciais e reservados e de informações de valor legal, devem obedecer aos prazos estabelecidos em lei ou regulamentos, conforme sua natureza;
- Ocorrendo situação em que os documentos confidenciais e reservados com informações ultrassecretas, secretas e reservadas não sejam mais oportunos, aqueles deverão ser destruídos conforme as seguintes orientações:
  - Não poderão ser descartados documentos confidenciais e reservados de valor histórico permanente;
  - Documentos eletrônicos confidenciais e reservados armazenados em servidores, após a sua exclusão, devem ser eliminados também dos locais de armazenamento temporário, mantidos pelos sistemas operacionais, a exemplo de lixeiras, quando existirem;
  - Documentos confidenciais e reservados eletrônicos, impressos ou armazenados em mídias transportáveis, reutilizáveis ou não, devem ser triturados em equipamento apropriado.

6.1.9. Na etapa de criptografia

É vedado o uso de qualquer sistema de cifra ou dispositivo de criptografia que não esteja de acordo com as prescrições corporativas definidas pela ASTIG e aprovadas pela Presidência da Companhia.

6.2. Tratamento a ser observado nas diversas etapas de tramitação de documentos públicos

6.2.1. Na etapa de recebimento

Cabe aos responsáveis pelo recebimento de documento públicos:

- Verificar, e registrar se for o caso, indícios de violação ou de quaisquer irregularidades na correspondência recebida, dando ciência do fato ao remetente;
- Assinar e datar o respectivo recibo que acompanha o documento, se houver;

- Proceder ao protocolo ou registro do documento em livro ou software adequado a tal finalidade, se necessário;
- Documentos eletrônicos em mídia transportável deverão ser submetidos a software antivírus, rejeitando-os quando verificada a sua existência, dando ciência do fato ao remetente.

6.2.2. Na etapa de elaboração
- Documentos públicos devem ser elaborados, preferencialmente, nas instalações da Companhia.
- Não é permitida a elaboração de documentos em lugares públicos.

6.2.3 Na etapa de manuseio
Documentos públicos podem ser manuseados livremente.

6.2.4 Na etapa de reprodução
É permitida a reprodução de todo ou parte de documento público.

6.2.5. Na etapa de divulgação
Documentos públicos podem ser divulgados para o ambiente externo, desde que, em havendo, sejam respeitadas as restrições ou formalidades para liberação, estabelecidas pela Companhia.

6.2.6 Na etapa de guarda
Documentos públicos, inclusive os gerados em meio magnético, devem ser guardados de forma a permitir a consulta posterior.

6.2.7 Na etapa de transporte
Os documentos públicos podem ser transportados livremente.

6.2.8. Na etapa de descarte
- O descarte de documentos e informações de valor legal, classificados como públicos, devem obedecer aos prazos estabelecidos em lei, conforme sua natureza;
- Não poderão ser descartados documentos corporativos com valor histórico permanente.

6.2.9. Na etapa de criptografia
É desaconselhável o uso de criptografia em documentos públicos.

6.3 Penalidades
O tratamento indevido de documentos será considerado falta grave e implicará na aplicação das sanções administrativas ou contratuais correspondentes, de acordo com a regulamentação interna vigente, bem como a legislação aplicável ao caso.

6.4 Competência para Classificação

6.4.1. Competência para classificação de informações
- **Ultrassecretas, secretas e reservadas** – Conselho de Administração e Diretoria Executiva;
- **Públicas** – Diretoria Executiva e Gestores, tanto para informações de impacto abrangente, como para aquelas de impacto local, consideradas, neste último caso, as diretrizes da Companhia para comunicação institucional e de relacionamento.

6.4.2. A Companhia deverá, uma vez identificada a informação, encaminhar a proposta de classificação ao Comitê Gestor de Acesso à Informação e ao Conselho Estadual de Acesso à Informação, para deliberação sobre o assunto.

6.5 Premissas Básicas

São premissas básicas para a gestão e divulgação de informações:

- Ao atribuir um grau de sigilo, a Companhia deve buscar um equilíbrio entre a necessidade de sigilo e os custos das medidas de proteção. Um grau de sigilo exagerado compromete a velocidade de transmissão da informação e contribui para a saturação dos sistemas de processamento e o desperdício nos recursos. Um grau de sigilo inferior ao adequado gera vulnerabilidades para o negócio;
- A classificação de uma informação deve ser preservada pelo prazo imposto por lei ou até atingir a obsolescência, após o que deve ser submetida a procedimentos de arquivo ou descarte;
- Uma informação poderá ter o seu grau de sigilo modificado. Neste caso, o gestor da informação deve ser alertado para a adoção das medidas de proteção decorrentes da mudança;
- Caso algum Gestor julgue que a classificação de uma informação seja inadequada, a nova classificação deve ser proposta, aumentando-se ou diminuindo-se a respectiva classificação, remetendo-a, se necessário, para a apreciação da autoridade classificadora original;
- A classificação da informação deve estar identificada e de fácil visualização;
- As informações da Companhia devem ser consideradas como corporativas;
- O acesso a informações ultrassecretas, secretas e reservadas só será admitido aos usuários que, no exercício de função ou atividade, tenham a necessidade de conhecê-las;
- Considerando o grau de sigilo, os gestores devem especificar formalmente os usuários das informações sob sua responsabilidade;
- Compete aos gestores, em suas respectivas áreas de atuação, organizar o conjunto de informações classificáveis como ultrassecretas, secretas e reservados ou Pública.

6.6 Responsabilidade e Desenvolvimento da Política

6.6.1 Conselho de Administração

Na condição de integrante da Administração da Companhia, é responsável pelas atualizações da Política de Segurança da Informação.

6.6.2. Diretoria Executiva

Na condição de integrante da Administração da Companhia, é responsável por encaminhar ao Conselho de Administração as propostas de atualização da presente Política de Segurança da Informação da Companhia, bem como por implantar e garantir o cumprimento da mesma nos diversos níveis da Organização.

Além disso, a Diretoria Executiva possui as seguintes responsabilidades inerentes à Segurança da Informação:

- Coordenar, orientar e avaliar as atividades relativas à Segurança da Informação na Companhia, promovendo ações de interesse corporativo;
- Estabelecer e manter atualizadas as normas, as diretrizes, os procedimentos e outros documentos relacionados à aplicação da presente Política, sempre que possível em articulação com as partes interessadas;
- Promover programas educacionais e de comunicação relacionados à Segurança da Informação na Companhia;

- Promover auditorias para verificar o cumprimento da política, das normas, das diretrizes, dos procedimentos e outros documentos de Segurança da Informação;
- Acompanhar as ações adotadas pelas áreas da Companhia para investigação e apuração de incidentes relativos a Segurança da Informação;
- Acompanhar estudos de implantação de novas tecnologias e seus possíveis impactos no que tange a Segurança da Informação.

6.6.3 Gestores

As responsabilidades dos ocupantes de todos os cargos de gestão no que tange à Segurança da Informação são as seguintes:

- Assessorar a Diretoria Executiva nas questões relativas à Segurança da Informação;
- Garantir o cumprimento da Política de Segurança da Informação, bem como das normas, diretrizes e procedimentos a ela relacionados, por parte dos usuários sob sua responsabilidade;
- Divulgar a Política de Segurança da Informação na Companhia e implantar as orientações da Diretoria Executiva em todas as unidades da Companhia;
- Coordenar programas de identificação, educação e conscientização de usuários de sua área de atuação;
- Coordenar a identificação de vulnerabilidades da sua área e a implantação de um plano de segurança da informação para solucioná-las, relatando à Diretoria Executiva as ocorrências e as práticas relevantes;
- Avaliar a eficácia da Segurança da Informação na sua área, reportando à Diretoria Executiva os resultados;
- Garantir a inclusão de cláusulas contratuais que assegurem a observância desta Política de Segurança da Informação;
- Aplicar as ações corretivas e disciplinares nos casos de quebra de segurança de informações por usuários sob sua responsabilidade;
- Informar as movimentações de usuários sob sua responsabilidade aos gestores e custodiantes;
- Reportar à Diretoria Executiva as situações que possam comprometer a segurança das informações da Companhia.

6.6.4. Gestores de Segurança da Informação

São denominados Gestores de Segurança da Informação os gerentes de cada área onde existe produção de informações cujas responsabilidades incluem:

- Identificar e classificar as informações sob sua responsabilidade;
- Definir as necessidades de segurança para as informações sob sua responsabilidade;
- Assegurar a adoção de medidas adequadas de segurança das informações sob sua responsabilidade;
- Conceder as autorizações de acesso às informações sob sua responsabilidade;
- Garantir que os custodiantes tenham pleno conhecimento desta Política e das necessidades de segurança para as informações sob sua responsabilidade;
- Participar da elaboração do plano de prevenção e recuperação das informações sob sua responsabilidade, para situações de contingência;
- Solicitar a aplicação de ações corretivas e disciplinares ao gestor do usuário responsável pela quebra de segurança de informações sob sua responsabilidade;
- Infórmar a Diretoria Executiva sobre situações que comprometam a segurança das informações sob sua responsabilidade.

6.6.5. Usuários

As responsabilidades dos Usuários relativas à Segurança da Informação são:

- Cumprir a Política de Segurança da Informação da Companhia;

- Reportar ao gestor imediato sobre situações que possam comprometer a segurança das informações da Companhia.

6.6.6. Auditoria (Interna ou Externa)

A Auditoria, interna ou externa, relativa a Segurança da Informação será determinada periodicamente pela Presidência, e terá por objetivo informar sobre a existência de situações que possam, de alguma forma, comprometer a segurança das informações da Companhia.

6.7 Disposições Gerais

A presente Política de Segurança da Informação da METROFOR será complementada por diretrizes, normas, procedimentos e outros documentos, considerados partes integrantes desta Política, e cuja competência de aprovação é da Diretoria Executiva.

6.8 REGISTROS

Identificação	Armazenamento	Grau de Sigilo	Proteção	Recuperação	Retenção	Disposição
Política de Gestão da Informação	Meio Eletrônico/ físico	Corporativo	Back up/pasta	Nome	Indeterminado	Não aplicável (N/A)

Versão	Data	Histórico	Aprovação
00		Emissão de Documento	

7. ANEXOS

Não aplicável.

Fernando Antonio Costa de Oliveira
Diretor - Presidente
METROFOR

Plinio Pompeu de Saboya M. Neto
Diretor de Operação e Manutenção
METROFOR

Francisco Edilson Ponte Aragão
Diretor de Desenvolvimento e Tecnologia
METROFOR

Giselle de Negreiros Secundino Frota
Diretora de Desenvolvimento Estratégico
Metrô de Fortaleza

José Tupinambá Cavalcante de Almeida
Diretor de Gestão Empresarial
Metrofor